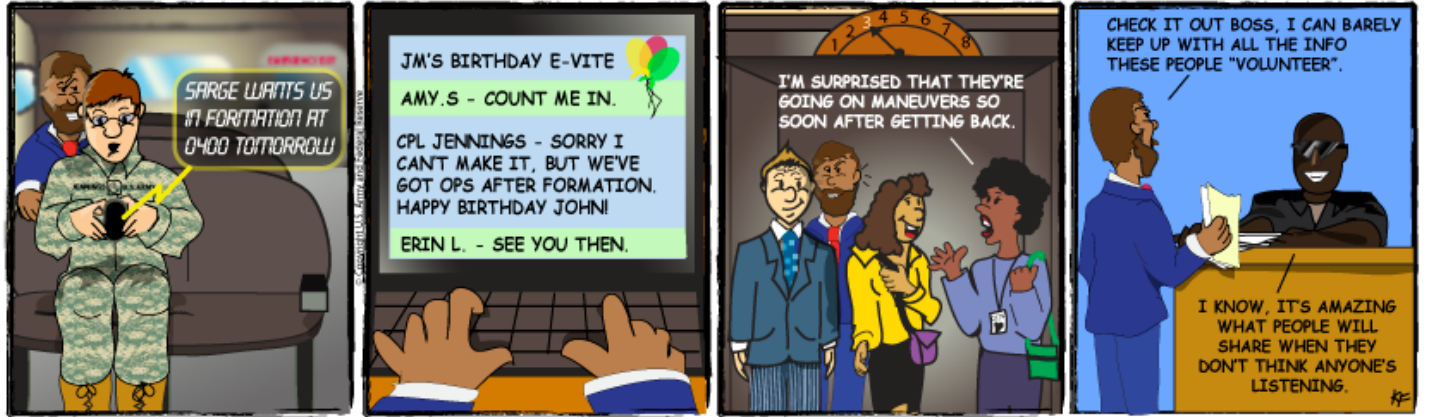


Think OPSEC

June 2012



ON CYBER PATROL



Once upon a time the US was known as the “Melting Pot of the World” because people from every corner of the globe would flock here to start a new life. You can see this every day as you walk down the street, ride public transportation or even shop at your local mall. Many times you will overhear people having a conversation in their native tongue and find it fascinating. “What exciting tales are they sharing” and “what language is that” are just some of the possible thoughts that may cross through your mind. As you overhear their conversation and wonder what information these two friends are sharing in their native language you should think how many times someone has overheard you speaking.

Operational Security (OPSEC) is a key element in keeping our country, soldiers, friends and family members safe. OPSEC, is keeping potential adversaries from discovering our critical information. As the name suggests, it protects our operations – planned, in progress, and those completed. Success depends on secrecy and surprise, so the military can accomplish the mission faster and with less risk. Our adversaries want our information, and they don’t concentrate exclusively on soldiers to get it. There are many ways our adversaries attempt to gain information in order to get an advantage. It is the responsibility of the individual to be watchful of their surroundings from both verbal eavesdropping and electronic monitoring.

With the many advances in technology that we enjoy it is very difficult to be out of contact these days. Most smart phones today offer the ability to surf the internet and send text messages all while carrying on a conversation. How many times have you found yourself on a crowded bus, train or other transportation while using your phone to send text messages? In those close proximities you never know how many people may be peaking over your shoulder as you discuss formation times, unit movements or the status of sensitive equipment. Sending a text informing someone that your unit is flying out the next morning may be all the enemy needs to know. A text about formation times and locations will provide a smart enemy with information needed to cause a great deal of damage to a large gathering of military personnel.

Have you ever received an invite to a party or event to a local hotspot and been prompted to reply online? You can see all the attendees as they update their status. Many list not only their intention on attending but also their reason for not making the event. The replies are available to everyone on the invite list, those you know and those you don’t. What would be the consequences when some unsuspecting Soldier posts that he or she can’t make the party because they have a military exercise early the next morning? It is hard to guess, but what is certain is that everyone who views the invite list will know. Our enemies surf the internet and focus on chat rooms and websites frequented by military

members. Many people have the town they live in included with their profile so any curious onlooker would know there is a military exercise happening the next morning.

There are many ways to gather information over the internet. Geotagging, the process of adding geographical information to various media, provides the exact location. Tweeting your location also provides a tracking mechanism and has gotten some Soldiers into trouble. Social media interactions are also a serious concern. Leaders must warn their Soldiers just as service members must warn their family members about the dangers in discussing sensitive information. Sometimes we assume everyone around us is a good guy based upon our location. Many times we let our guard down when we speak in a cleared location because we assume everyone around us is on our side. How often have you overheard two people carrying on a conversation in an elevator in a secured building? They assume everyone is okay because the building is guarded and everyone has a clearance. Many times there are vendors, visitors or facility personnel carrying on their daily business within earshot of our offices.

Many times we are not paying attention to who is paying attention to us, yet we notice those talking loud on a plane or sharing too much personal information all the time. While we are watching and listening to those obvious conversations we must also ensure no one is attempting to gain access to our information. Leaders must discuss with their teams on the importance of keeping vigilant and guarding our conversations whether they are conducted in person, in electronic media or over the phone.

We must always remain diligent and be aware of our surrounding.